Department of Homeland Security Daily Open Source Infrastructure Report for 31 March 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports authorities allege that three teenagers broke into a Blackstone, Massachusetts, water storage facility after cutting barbed wire and slicing the lines to an alarm, highlighting the vulnerabilities of municipal water supplies. (See item 20)
- The New York Times reports scientists question effectiveness of bird−flu vaccine since it protects only about half the people who receive it. (See item 23)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 29, United Press International* — **Oil pipeline maintenance improved.** U.S. lawmakers are scrambling to review whether pipeline operators are complying with maintenance regulations ahead of the expiration of a key pipeline safety act. The Pipeline Safety and Security Act, which is geared toward improving the well being of 2.2 million miles of U.S. pipelines, was passed and signed into law in November 2002. It mandated the inspections of half of all interstate gas pipelines within five years; the rest faced initial inspections within a decade. With an expiration date pending for later this year, legislators are assessing the worth of the legislation and operators note that the upkeep of the pipelines is their top concern. Operators spend $8,000 a mile on maintenance of pipelines, said Raymond Paul of

the Association of Oil Pipelines. He said there was still much work to be done at the state level on education and enforcement in providing support for damaged pipelines.
Source: http://www.upi.com/Energy/view.php?StoryID=20060327−124149−7 594r

2. *March 29, Leavenworth Times (KS)* — **Emergency responders learn about pipeline hazards.** When responding to a pipeline hazard involving burning natural gas or the leak of some other dangerous substance, first responders may think they can solve the problem by turning a nearby valve. But local firefighters and other emergency officials were cautioned against this Tuesday, March 28 because some pipeline companies may have the ability to control the valves from a station miles away. And first responders could make the problem worse by turning on a valve that has already been shut off. This was one of the tips provided during a pipeline safety and incident response training session at Leavenworth Fire Station No. 1 in Kansas. The training included information about leak recognition, damage prevention, and how to safely respond to an incident. O.G. McClinton Jr. of the Pipeline Safety Institute said it is important for emergency responders to understand where the pipelines are located, the type of products, the pressure levels, whether the substances are odorized, and the response times of the pipeline operators.
Source: http://www.leavenworthtimes.com/articles/2006/03/29/news/new s04.txt

3. *March 29, Associated Press* — **Venezuelan: Exxon Mobil not welcome.** Venezuela's oil minister said Wednesday, March 29 that Exxon Mobil was no longer welcome in this oil−producing nation. Exxon Mobil has resisted government tax increases and contract changes to "re−nationalize" the oil industry. Rather than submit to new terms that will turn 32 privately run oil fields over to state control, the company sold its stake in the 150,000 barrel−a−day Quiamare−La Ceiba field to Spanish−Argentine major Repsol YPF. In February, state oil company Petroleos de Venezuela SA ousted Exxon from a multibillion dollar petrochemicals project. The Texas company still holds a 41.7 percent stake in the 120,000−barrel−a−day Cerro Negro heavy oil upgrading project in the Orinoco belt. Also, Exxon Mobil and Canadian oil and gas company PetroCanada each hold a 50 percent stake in the La Ceiba field. Venezuela is the world's fifth largest oil exporter and a main source of U.S. oil imports.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/29/AR2006032902717.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *March 30, KETV 7 (NE)* — **Truck spills diesel on interstate in Nebraska.** A truck carrying diesel fuel and traveling along Interstate 80 in Omaha, NE, spilled about 100 gallons of its load Thursday morning, March 30. Although this incident occurred in rush hour traffic, no one was injured.
Source: http://www.ketv.com/newsarchive/8358283/detail.html

[Return to top]

Defense Industrial Base Sector

5. *March 30, National Defense Magazine* — **Marines struggle to begin rebuilding force.** The Marine Corps is requesting a budget of $18.2 billion for 2007, but only a fraction of that will go to buy new equipment, said Lt. General Emerson N. Gardner, deputy commandant for programs and resources. The Corps will need nearly $10 billion in additional funds from two separate 2006 supplemental appropriations to help the service begin to recover from the Iraq war and reorganize for an extended campaign against terrorism, said Gardner. The Marines already have received one bridge supplemental appropriation of $4.1 billion, part of a larger measure that President Bush signed into law in December. A second supplemental request, sent to Capitol Hill in February, contains another $5.7 billion for the Corps. Both of those supplements are necessary for the Marines to continue operating with the current level of troops and equipment in the coming year, Gardner asserted. Although the $18.2 billion is up slightly from the $17.5 billion the Corps sought in 2006, only $1.4 billion −− less than 10 percent −− will go to procure new equipment, Gardner explained. For this reason, the supplements are essential in paying for repairing and replacing lost or damaged equipment, Gardner said.
Source: http://www.nationaldefensemagazine.org/issues/2006/april/mar inesstruggle.htm

6. *March 30, National Defense Magazine* — **War supplementals have morphed traditional military budgeting and spending.** A combination of bigger procurement accounts in this year's budget and war−emergency appropriations puts the Army on course to receive some of the largest levels of funding it has seen in decades. The most recent budget proposal is indicative of a continuing trend that points to substantial procurement spending included in supplemental requests. Soaring equipment expenditures, to a great extent, are the consequence of three years of fighting in Iraq with more than 100,000 soldiers on the ground. But much of the new hardware, Army officials note, also is needed to make up shortages that started after the end of the Cold War. By the Army's own account, the shortfalls add up to a staggering $100 billion. War supplementals have changed the traditional dynamics of military budgeting and spending. For the Army, which has shouldered the lion's share of the deployment duties in Iraq and Afghanistan, the additional appropriations have allowed unprecedented flexibility in balancing its resources.
Source: http://www.nationaldefensemagazine.org/issues/2006/april/mus cle.htm

7. *March 30, Government Accountability Office* — **GAO−06−604T: Defense Logistics: Preliminary Observations on Equipment Reset Challenges and Issues for the Army and Marine Corps (Testimony).** The United States is engaged in an unconventional war, not a war against military forces of one country, but an irregular war against terrorist cells with global networks. Operations Iraqi Freedom and Enduring Freedom are sustained military operations, which are taking a toll on the condition and readiness of military equipment that, in some cases, is more than 20 years old. The Army and Marine Corps will likely incur large expenditures in the future to reset (repair or replace) a significant amount of equipment when hostilities cease. The Army has requested about $13 billion in its fiscal year 2006 supplemental budget request for equipment reset. This testimony addresses (1) the environment, pace of operations, and operational requirements in Southwest Asia, and their affects on the Army's and Marine Corps's equipping and maintenance strategies; (2) equipment maintenance consequences created by these equipping and maintenance strategies; and (3) challenges affecting the timing and cost of Army and Marine Corps equipment reset. The Government Accountability Office's (GAO) observations are based on equipment−related GAO reports issued in fiscal years 2004

through 2006, as well as ongoing related work.
Highlights: http://www.gao.gov/highlights/d06604thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−604T

[Return to top]

Banking and Finance Sector

8. *March 29, Department of State* — **FBI works to protect global citizens from online crime.** The Internet Crime Complaint Center (IC3) is a reporting and referral system for Internet crime complaints. Through an online complaint form and a team of agents and analysts, IC3 serves the U.S. and international law enforcement agencies investigating cyber crime. Six federal agents and approximately 40 analysts receive Internet−related criminal complaints from the public, then research, develop, and refer the complaints to law enforcement or regulatory agencies and multi−agency task forces for investigation. IC3 takes an individual citizen's complaint and combines it with information from other victims around the world who have lost money in the same scenario, and builds that into a substantial case. The Cyber Initiative and Resource Fusion Unit (CIRFU) eliminates false leads and refines a case before it is referred to enforcement agencies or task forces. When the CIRFU hears of a specific trend or problem, the unit targets the top offenders and learns more about how they operate. IC3 informs the public about the trends and scams through a public service advisory or alert posted on the IC3 Website or disseminated in other ways.
IC3 Website: http://www.ic3.gov
Source: http://usinfo.state.gov/xarchives/display.html?p=washfile−english&y=2006&m=March&x=20060329162436cmretrop3.617495e−02&t= gi/gi−latest.html

9. *March 29, Newsday* — **Release of teachers' Social Security numbers being reviewed.** The Connecticut state Department of Education disclosed the Social Security numbers of about 1,250 teachers and administrators in Connecticut's vocational−technical schools in an e−mail this week, state officials said Wednesday, March 29. Attorney General Richard Blumenthal said his office will investigate. The numbers were included in an e−mail sent Monday, March 27 by a state consultant to principals and assistant principals at the state's 17 technical high schools, two satellite schools, and a technical education center, according to the union representing those teachers. Aaron Silvia, of the State Vocational Federation of Teachers, said the e−mail was then forwarded to some teachers, further spreading the Social Security numbers.
Source: http://www.newsday.com/news/local/wire/connecticut/ny−bc−ct−−teacherinfo0329mar29,0,2153656.story

10. *March 29, eWeek* — **ID theft bill readies for a vote.** The federal House Committee on Energy and Commerce has approved an identity theft bill that would set a national standard for data brokers' efforts to protect personal information. The Data Accountability and Trust Act was nearly one year in the making, following several high−profile data security breaches last year. The act would require data brokers to institute a security policy for collecting, using, selling and securing the information they hold, and they would be required to monitor their security systems regularly. If a breach occurs, the Federal Trade Commission (FTC) or an independent auditor would review the broker's security plan following a breach, and subsequently the FTC would be permitted to require audits for five years. If there is a reasonable risk of ID theft,

fraud or unlawful conduct as a result of a breach, the company would have to notify U.S. consumers whose data was acquired by an unauthorized person as a result of the breach. The company would have to notify the FTC and post a notice on its Website. The bill also would make it illegal for brokers to obtain data on someone by impersonating that person, a practice known as "pretexting."
Source: http://www.eweek.com/article2/0,1895,1944086,00.asp

11. *March 29, IDG News Service* — **Florida banks hacked in new spoofing attack.** Three Florida banks have had their Websites compromised by hackers in an attack that security experts are calling the first of its type. Earlier this month, attackers were able to hack servers run by the Internet service provider that hosted the three banks' Websites. They then redirected traffic from the legitimate Websites to a bogus server, designed to resemble the banking sites, according to Bob Breeden of the Florida Department of Law Enforcement's Computer Crime Center. Users were then asked to enter credit card numbers, PINs, and other types of sensitive information. According to Breeden, the affected banks are Premier Bank, Wakulla Bank, and Capital City Bank, all small regional banks based in Florida. This attack was similar to phishing attacks that are commonly used against online commerce sites, but in this case hackers had actually made changes to legitimate Websites, making the scam much harder for regular users to detect. This attack worked on users who had typed in the correct URL for the banks in question. Breeden said he had not seen this particular tactic used before. He said the technique appeared to be very effective at extracting sensitive information.
Source: http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,110046,00.html

12. *March 27, Better Business Bureau* — **Better Business Bureau launches national initiative to help small businesses protect customer and employee data.** The Council of Better Business Bureaus (BBB) and Privacy & American Business on Monday, March 27 unveiled a new national education initiative geared toward helping small business owners improve their security and privacy readiness in a climate of data exposure risks. The BBB's initiative is designed to demystify the complexities of data security and give small businesses a non−technical roadmap to securing their customer data. The national program includes free, easy−to−read security and privacy toolkits, with separate kits focused on customer and employee data protection. The high profile data breaches at major corporations have largely eclipsed small business vulnerabilities. Yet, a 2005 survey by the Small Business Technology Institute reports that more than half of all small businesses in the U.S. experienced a security breach in the last year. Nearly one−fifth of small businesses do not use virus−scanning software for e−mail, over 60 percent do not protect their wireless networks with encryption, and two−thirds of small businesses do not have an information security plan, according to the study. Small businesses, overall, make reactive purchase decisions in relation to information security, and usually purchase products only after suffering an information security incident.
Educational materials: http://www.bbb.org/securityandprivacy
Source: http://www.bbb.org/alerts/article.asp?ID=666

[Return to top]

Transportation and Border Security Sector

13. *March 30, Associated Press* — **New Orleans airport's recovery at 50 percent.** Seven months after Hurricane Katrina, New Orleans' international airport is at more than 50 percent of its pre−storm passenger levels, airport officials say. Passenger traffic in February at Louis Armstrong International Airport was down 48 percent from a year ago. In February, nearly 427,000 passengers passed through the airport, compared to almost 835,000 in February 2005. More flights are being added, said airport spokesperson Michelle Duffourc.
Source: http://www.usatoday.com/travel/flights/2006−03−29−nola−airpo rt_x.htm

14. *March 30, Associated Press* — **Venezuela suspends ban on U.S. airlines.** The Ministry of Infrastructure said in a statement late Wednesday that April 25 was the new deadline by which the U.S. Federal Aviation Administration (FAA) must drop restrictions against Venezuelan carriers or face the retaliatory measure. That would give time for FAA officials in Caracas this week time to finish their safety audit of the country and upgrade Venezuela's safety ranking, it said. Caracas is protesting the FAA's Category 2 safety ranking of Venezuela, imposed in 1995, which has prohibited Venezuelan airlines from flying their own planes to the United States or from launching new services such as expansions or changes in routes.
Source: http://biz.yahoo.com/ap/060330/venezuela_us_airlines.html?.v =3

15. *March 30, Detroit Free Press* — **NWA plans June start for new carrier.** In two months, Northwest Airlines (NWA) wants to launch its new subsidiary, a commuter carrier called Compass Airlines, to fly passengers to its hubs −− Detroit, Minneapolis, and Memphis −− and a network of small and midsize cities. Compass' inaugural route will fly passengers between Minneapolis and Washington, DC, in June, with plans for further expansion starting in March 2007, according to documents filed this week with the Department of Transportation. As a commuter carrier, Compass stands to have a major presence at Detroit Metro Airport, where Northwest's current commuter carriers, Mesaba Airlines and Pinnacle Airlines, handle about 225 daily flights, or 44 percent of Northwest's 510 flights a day there. Compass will operate a portion of Mesaba's flights and is part of Northwest's plan to replace its fleet of DC9s, which average more than 30 years old. The commuter will lower labor costs for Northwest because its pay scale will be lower than Northwest's wage structure.
Source: http://www.usatoday.com/travel/flights/2006−03−30−nwa−carrie r_x.htm

16. *March 30, Daily Press (VA)* — **Container cargo could end up out in the country.** As Asian imports continue to stream into U.S. ports in greater numbers, the Hampton Roads commercial real estate community is keying in on the need for warehouse and distribution space before transporting those goods inland. A consultant for the Virginia Port Authority predicts that an increase in container traffic over the next 25 years will require 20 million to 60 million more square feet of warehouse and distribution center space. That compares with the region's 10 million to 15 million square feet dedicated to that use now. Most of the region's cargo is headed west. And most of the land around the terminals in Norfolk, Portsmouth, and Newport News is developed. So commercial developers are looking increasingly at the farmland along primary highways and rail routes in Suffolk and Isle of Wight County for new buildings. The trend toward this kind of development represents a sea change of sorts, as more development is geared toward getting goods manufactured abroad into the United States. "My fear, as an engineer, is gridlock," Mike Crist said. He's an engineer with Moffatt & Nichol, the firm that has worked with the Port Authority to study the need for more distribution center space.
Source: http://www.dailypress.com/business/local/dp−95877sy0mar30,0,

7464108.story?coll=dp−business−localheads

17. *March 30, Government Accountability Office* — **GAO−06−591T: Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System (Testimony).** U.S. Customs and Border Protection's (CBP) Automated Targeting System (ATS)—a computerized model that CBP officers use as a decision support tool to help them target oceangoing cargo containers for inspection— is part of CBP's layered approach to securing oceangoing cargo. The Government Accountability Office (GAO) reported in February 2004 on challenges CBP faced in targeting oceangoing cargo containers for inspection and testified before this subcommittee in March 2004 about the findings in that report. The report and testimony outlined recommendations aimed at (1) better incorporating recognized modeling practices into CBP's targeting strategy, (2) periodically adjusting the targeting strategy to respond to findings that occur during the course of its operation, and (3) improving implementation of the targeting strategy. This statement for the record discusses preliminary observations from GAO's ongoing work related to ATS and GAO's 2004 recommendations addressing the following questions: 1. What controls does CBP have in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of smuggled weapons of mass destruction? 2. How does CBP systematically analyze security inspection results and incorporate them into ATS? 3.What steps has CBP taken to better implement the rest of its targeting strategy at the seaports?
Highlights: http://www.gao.gov/highlights/d06591thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−591T

18. *March 29, USA TODAY* — **Canadian pilots say traction tests beat U.S. system.** The fatal accident in December at Chicago's Midway International Airport is focusing new attention on safety at airports during winter months, when runways can become dangerously slippery. Canada, prompted by its own fatal crash in 1989, already has such a system. Airports have a numerical rating of a runway's slickness, known as the Canadian Runway Friction Index. That information is passed on to pilots, who use it to calculate how much distance they need to stop after touchdown. Though the process varies slightly at different airports, the routines are similar. A pickup truck driver goes up one side of the 10,000−foot main runway, locking the brakes 10 different times. Each time he brakes, a device known as an MK 3 Electronic Decelerometer measures traction. Then he drives the other direction on the runway, performing 10 more tests. The Federal Aviation Administration (FAA), which regulates airports in the U.S. helped fund research that Canadians used to establish their system, but the FAA has been wary of adopting it. FAA officials say there is too much room for error in the Canadian system.
Source: http://www.usatoday.com/travel/flights/2006−03−28−canada−run way−tests_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

Nothing to report.

[Return to top]

Food Sector

19. *March 30, Agricultural Research Service* — **Sorter can tell the difference between clean kernels and those ruined by insects.** Thomas Pearson, a scientist with the Agricultural Research Service (ARS), has developed an acoustics−based sorter that can distinguish between "clean" wheat kernels and those that have been nibbled on and spoiled by insects. The idea behind the novel technology is simple. A wheat kernel that's whole and intact will make a slightly different, high−pitched "ping" when striking a steel plate than the sound made by a kernel that's been tunneled through by an insect. After assessing the kernels' acoustic qualities, the sorter will shunt the insect−damaged wheat kernels from a random sample into one bin, and send "acceptable" kernels into another. It can even pinpoint kernels with tiny insect larvae hiding inside them, a feat that, for grain inspectors, is like trying to find a needle in a haystack. Every year, more than $1.5 billion worth of U.S. wheat and other grains must be discarded or downgraded because of post−harvest damage by insect pests. Despite preventive measures, the pests—ranging from moth larvae to small flour beetles—still manage to find their way into grain storage facilities.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

20. *March 30, Associated Press* — **Breach at water tank shows vulnerabilities.** Authorities allege that three teenagers had broken into a Blackstone, MA, water storage facility after cutting barbed wire and slicing the lines to an alarm. Authorities ruled out terrorism, but the breach in the town of 9,000 highlighted the vulnerabilities of municipal water supplies. Authorities said Wednesday, March 29, that tests found no evidence of chemical contamination in the water. But the damage already was done: Schools and businesses were closed, use of water for any purpose was banned, residents had been put on edge and thousands of dollars were spent on tests and repair. While water is not a spectacular target for vandals or terrorists when compared with a nuclear plant or giant sports stadium, towns depend on it for drinking, bathing, business and firefighting.
Source: http://www.twincities.com/mld/twincities/news/breaking_news/ 14216860.htm

21. *March 29, Associated Press* — **Hospital flushes water system.** A hospital's water system had to be boiled and flushed after an elderly patient contracted Legionnaire's disease. Ellis Hospital in Schenectady, NY, was given a clean bill of health Tuesday, March 28, by the state Department of Health, after the bacteria that causes the disease was eradicated. For four days, patients and workers on two hospital wings used bottled water and took sponge baths while waiting for the water to be decontaminated. Legionnaire's disease is a form of pneumonia caused by bacteria that occur naturally in water.
Source: http://www.capitalnews9.com/content/top_stories/default.asp? ArID=173842

[Return to top]

Public Health Sector

22. *March 30, Agence France−Presse* — **H5N1 found in southern Russian province.** The H5N1 strain of bird flu virus has been found among dozens of dead birds in Russia's southern province of Volgograd, officials in the province said. Preventive work including disinfection is being carried out and two million doses of a bird flu vaccine have been sent to the province from Moscow, the statement said. Russia's chief veterinarian warned last week that bird flu was posing a growing threat to the country. "Last year the virus affected 62 towns in 10 Russian regions, while since the start of 2006, already 56 towns in nine regions have been affected," Sergei Dankvert said at a veterinarians' conference.
Source: http://news.yahoo.com/s/afp/20060330/hl_afp/healthflurussia_060330095518

23. *March 29, New York Times* — **Scientists question effectiveness of bird−flu vaccine.** A bird−flu vaccine being stockpiled by the government in preparation for a possible pandemic protects only about half the people who receive it, scientists are reporting. In addition, it must be given in such high doses that if a pandemic were to start soon, manufacturers could not begin to make enough vaccine for all who would need it. A dose 12 times the amount used in a standard flu shot protected just 54 percent of the people. Initial findings from the same study were first announced in August. At that time, researchers were thrilled to have a vaccine that worked at all. The new report is the first to include results on all the participants, 451 adults from 18 to 64 who were inoculated at three medical centers in the U.S. They received two shots a month apart. No serious side effects occurred, though some got sore arms from the shots. The vaccine was developed by government and other researchers, and is being made by Sanofi Pasteur under a government contract. It is designed to prevent the disease caused by the (A)H5N1 avian flu virus that has been spreading rapidly through Asia, Europe and Africa.
Safety and Immunogenicity of an Inactivated Subvirion Influenza A (H5N1) Vaccine:
http://content.nejm.org/cgi/content/full/354/13/1343
Source: http://www.nytimes.com/2006/03/29/health/29cnd−vaccine.html?_r=1&oref=slogin

24. *March 29, U.S. Food and Drug Administration* — **Second drug for the prevention of influenza A and B approved.** The U.S. Food and Drug Administration (FDA) Wednesday, March 29, approved the use of Relenza (zanamivir for inhalation) for prevention (prophylaxis) of influenza in adults and children five years of age and older. Relenza, an antiviral medication, was previously approved for the treatment of influenza A and B virus infections in adults and children. Tamiflu (oseltamivir phosphate) previously was approved for both prevention and treatment of flu; this approval of Relenza for prevention provides Americans with another option for the prevention of influenza A and B infections.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01341.html

[Return to top]

Government Sector

25. *March 30, GovExec* — **Fire closes IRS headquarters.** The Internal Revenue Service's (IRS) headquarters building in Washington, DC, has been closed after an electrical fire Wednesday morning, March 29. The building, which is downtown on Constitution Avenue and houses more than 3,000 employees, was evacuated at about 9:30 a.m. EST, a spokesperson said. Employees were later told they could go back inside to collect personal belongings before heading home, she said. There have been no reports of injuries. According to an agency statement, the building remained closed because of the smoke and a lack of electrical power, but the spokesperson said the building's power was still on when she returned for her personal items.
Source: http://www.govexec.com/story_page.cfm?articleid=33715&dcn=to daysnews

26. *March 30, Government Accountability Office* — **GAO−06−573T: Polar−Orbiting Operational Environmental Satellites: Cost Increases Trigger Review and Place Program's Direction on Hold (Testimony).** Polar−orbiting environmental satellites provide data and imagery that are used by weather forecasters, climatologists, and the military to map and monitor changes in weather, climate, the oceans, and the environment. They are critical to long−term weather prediction, including advance forecasts of a hurricane‘s path and intensity. Our nation’s current operational polar−orbiting environmental satellite program is a complex infrastructure that includes two satellite systems, supporting ground stations, and four central data processing centers. In the future, the National Polar−orbiting Operational Environmental Satellite System (NPOESS) is to combine the two current systems into a single, state−of−the−art environment−monitoring satellite system. NPOESS is considered critical to the United States’ ability to maintain the continuity of data required for weather forecasting and global climate monitoring though the year 2020. The National Oceanic and Atmospheric Administration (NOAA), the Department of Defense (DOD), and the National Aeronautics and Space Administration (NASA) have formed a tri−agency integrated program office to manage NPOESS. The Government Accountability Office (GAO) was asked to determine the NPOESS program’s current status and plans and to discuss considerations in moving the program forward.
Highlights: http://www.gao.gov/highlights/d06573thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−573T

27. *March 29, Government Accountability Office* — **GAO−06−559T: Homeland Security: The Status of Strategic Planning in the National Capital Region (Testimony).** The Subcommittee asked the Government Accountability Office (GAO) to provide comments on the National Capital Region’s (NCR) strategic plan. GAO reported on NCR strategic planning, among other issues, in May 2004 and September 2004, testified before the House Committee on Government Reform in June 2004, and testified before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia in July 2005. In this testimony, we addressed completion of the NCR strategic plan, national and regional priorities, and strengthening any plan that is developed. Although GAO includes no new recommendations in this statement, GAO continues to recommend that the Office of National Capital Region Coordination work with the NCR jurisdictions to quickly complete a coordinated strategic plan to establish and monitor the achievement of regional goals and priorities.
Highlights: http://www.gao.gov/highlights/d06559thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−559T

[Return to top]

Emergency Services Sector

28. *March 30, Providence Journal (RI)* — **Rhode Island preparedness and security effort: New photo ID badges for employees.** Increasing numbers of Providence, RI, employees are toting new photo ID badges as part of a government effort to tighten security and be ready for crises. "You need to know, in the age of terrorism, who people are in city buildings," said Leo Messier, city director of emergency management and homeland security. Thanks to a federal Homeland Security grant, the city has obtained a portable badge−making system that it is using to create the permanent IDs. The system is designed to be used in a disaster, to quickly make badges for the people, including volunteer relief workers and victims, and better control the scene of the incident and coordinate the response. If there is an incident and city employees other than uniformed emergency workers are called on, they will be easily distinguished by badges, Messier said. The system has proved itself already. When evacuees from Hurricane Katrina were relocated temporarily to Middletown, two city workers from Providence made photo ID badges in the field for the evacuees and Red Cross volunteers. The Providence Emergency Management Agency also tested it last summer in an evacuation drill at the Municipal Wharf.
Source: http://www.projo.com/ri/providence/content/projo_20060330_pr ovids.1d8800d.html

29. *March 29, Reuters* — **Lawmakers criticize Washington disaster plan delay.** The U.S. capital is vulnerable to a major terror attack or natural disaster because it still does not have a coordinated recovery plan, U.S. senators and other government officials said on Wednesday, March 29. A disaster response plan for Washington, DC, neighboring Virginia and Maryland, and the federal government that was due last September is still being worked on and will probably be nearly a year late, officials told a Senate Homeland Security and Governmental Affairs subcommittee. In joint testimony, emergency management officials from the District of Columbia, Maryland and Virginia said they hope to complete a final version of the emergency master plan by August.
Source: http://news.yahoo.com/s/nm/20060330/us_nm/security_washingto n_dc_1

30. *March 29, Congress Daily* — **Committee seeks changes in color−coded alert system.** The House Homeland Security Intelligence Subcommittee Wednesday, March 29, approved a bill designed to overhaul the nation's color−coded threat alert system and improve information sharing with state and local governments, tribal officials and the private sector. The bill would require the department to implement a new homeland security advisory system to disseminate information on threats and appropriate protective measures to state, local and tribal officials, and the private sector.
Source: http://www.govexec.com/story_page.cfm?articleid=33718&dcn=to daysnews

31. *March 29, Gallatin News Examiner (TN)* — **Tennessee to conduct regional disaster drill.** Sumner County, Metro Nashville, Williamson and Wilson counties in Tennessee will soon participate in an exercise, being conducted Friday and Saturday, April 7−8, designed to show just how prepared emergency and health officials are in the region to react to disasters, manmade or natural. Drills such as the one planned for April will not only test plans that are

already made, but point out what is needed for the future. “We are going to find out where we are and where we need to be to be ready,” said Sumner County Executive Hank Thompson. Possible scenarios may include a tornado or series of tornados, or an event involving weapons of mass destruction caused by a terrorist, according to Ken Weidner, director of Sumner County’s Emergency Management Agency.
For more information: https://www.hsd5exercise.org/Nashville/nashville.nsf/mainpage?OpenForm
Source: http://www.gallatinnewsexaminer.com/apps/pbcs.dll/article?AID=/20060329/MTCN0401/303290034/1310/MTCN04

32. *March 28, Government of Canada Newsroom* — **Canada conducts radiological incident exercise.** This week a team of technical experts from the Government of Canada are gathering at Slemon Park in Prince Edward Island to conduct a radiological incident exercise. More than 140 of Canada’s top radiological−nuclear experts will take part in Exercise Maritime Response, a three−day field exercise that will pit them against some of the toughest conditions ever experienced in this kind of field exercise. Participants will be trained on how to appropriately respond to terrorist attacks involving radiological−nuclear sources. This will be the first national level exercise of this kind ever held in Canada involving integrated teams.
Source: http://news.gc.ca/cfmx/view/en/index.jsp?articleid=203999

[Return to top]

Information Technology and Telecommunications Sector

33. *March 30, Register (UK)* — **Joe−job spammers shift tactics to evade filters.** Spammers are applying a new twist to joe−jobbing −− a trick used to get around e−mail filters. Instead of forging the sender's e−mail, as done in conventional joe−jobbing, address spammers are deliberately sending their messages to an invalid e−mail address at a high profile company using a forged "From" address at a target company. Because of this, the IP address and the e−mail domain address now match and the junk e−mail message may be able to surpass e−mail filters.
Source: http://www.theregister.co.uk/2006/03/30/joe_job_twist/

34. *March 29, Security Focus* — **RealNetworks multiple products multiple buffer overflow vulnerabilities.** Remote exploitation of a heap based buffer overflow in RealNetwork Inc.'s RealPlayer could allow the execution of arbitrary code in the context of the currently logged in user. Analysis: Successful exploitation allows a remote attacker to execute arbitrary code with the privileges of the currently logged in user. In order to exploit this vulnerability, an attacker would need to get a user to follow a link to a malicious server. For a list of vulnerable products: http://www.securityfocus.com/bid/17202/info
Solution: The vendor has released fixes to address these issues. See references for further details: http://www.securityfocus.com/bid/17202/references
Source: http://www.securityfocus.com/bid/17202/discuss

35. *March 29, eWeek* — **Latest Bagle worm has rootkit features.** Malicious hackers have fitted rootkit features into the newest mutants of the Bagle worm, adding a stealthy new danger to an

already virulent threat. According to virus hunters at F−Secure, of Helsinki, Finland, the latest Bagle.GE variant loads a kernel−mode driver to hide the processes and registry keys of itself and other Bagle−related malware from security scanners. The use of offensive rootkits in existing virus threats signals an aggressive push by attackers to get around existing anti−virus software and maintain a persistent and undetectable presence on infected machines. The Bagle threat started as a simple e−mail executable in 2004 but has grown and evolved over the years to become one of the most active threats against PC users. Security researchers estimate that the numerous Bagle variants have infected more computers than any other virus group.
Source: http://www.eweek.com/article2/0,1895,1944133,00.asp

36. *March 29, CNET News* — **Spy program snoops on cell phones.** New software, called FlexiSpy, released in March by Bangkok, Thailand−based Vervata, hides on cell phones and captures call logs and text messages. It is being sold as a way to monitor kids and spouses. The data captured is sent to Vervata's servers and is accessible to customers via a special Website. Security company F−Secure has labeled the software a Trojan. "This application installs itself without any kind of indication as to what it is," Jarno Niemela wrote on the Finnish antivirus maker's corporate blog Wednesday, March 29. In addition, FlexiSpy could be used by miscreants as part of malicious software that targets phones, Niemela wrote.
Source: http://news.com.com/Spy+program+snoops+on+cell+phones/2100−1029_3−6055760.html?tag=nefd.top

37. *March 29, Government Accountability Office* — **GAO−06−598T: Homeland Security: Progress Continues but Challenges Remain in Department's Management of Information Technology (Testimony).** Information technology (IT) is a critical tool for the Department of Homeland Security (DHS), not only in performing its mission today, but also in transforming how it will do so in the future. In light of the importance of this transformation and the magnitude of the associated challenges, the Government Accountability Office (GAO) has designated the implementation of the department and its transformation as high risk. GAO has reported that in order to effectively leverage IT as a transformation tool, DHS needs to establish certain institutional management controls and capabilities, such as having an enterprise architecture and making informed portfolio−based decisions across competing IT investments. GAO has also reported that it is critical for the department to implement these controls and associated best practices on its many IT investments. In its past work, GAO has made numerous recommendations on DHS institutional controls and on individual IT investment projects. The testimony is based on GAO's body of work in these areas, covering the state of DHS IT management both on the institutional level and the individual program level.
Highlights: http://www.gao.gov/highlights/d06598thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−598T

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in the following US−CERT Vulnerability Note:

VU#876678 − Microsoft Internet Explorer createTextRange() vulnerability
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#how_to _secure

We will continue to update current activity as more information becomes available.

Phishing Scams

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 26777 (−−−), 32459 (−−−), 41170 (−−−), 55763 (−−−), 55620 (−−−), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.